REMARKS

Introduction

Claims 1, 2, 4-18 and 20-25 were pending. Claims 1, 18, and 23 are independent. Claims 1, 18, and 23 have been amended.

Applicants note with appreciation the courtesies extended by Examiner Taylor during the telephonic interview conducted on October 31, 2007. In the interview, Examiner Taylor and Applicants' Agent Cappo discussed the possible reconsideration of independent claim 1 as being patentable. Agent Cappo and Examiner Taylor discussed that in the claimed invention, rules for restricting access to a call report are based not only on an employee's position within a company, but also on the matters the employee has worked on, as well as the matters that are within the employee's current responsibility, which further restrict access beyond the just the employee's position. Agent Cappo asserted that these further restrictions are not taught by any of the references cited in the prior office action. Examiner Taylor agreed that such extra restrictions may render claim 1 patentable after further study of Agent Cappo's written arguments, but asserted that claim 1 in its present form would not overcome the pending rejection because the added restrictions were placed within a wherein clause, to which the Examiner is not giving much weight. Agent Cappo offered a possible amendment to claim 1 which would remove the "wherein" clause and apply the further limitations directly to the rules for restricting access. Examiner Taylor agreed to reconsider the patentability of claim 1 if amended in this way. Applicant has herein amended claims 1, 18, and 23 in accordance with the discussions during the interview.

Rejections under 35 U.S.C. § 103(a)

Claims 1, 2, 4-18 and 20-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0176973 (Lapeze et al.) in view of U.S. Patent Application Publication No. 2002/0184527 (Chun et al.) and further in view of U.S. Patent Application Publication No. 2002/0107889 (Stone et al.).

Lapeze et al. describes a contact management and control system for managing contact events associated with an enterprise. The contact management system detects a contact event and actuates a contact manager to retrieve information pertaining to the contact event from a contact library. If new information is associated with the contact event, the contact library is updated with the new information. Information in the updated library is subsequently disseminated across the enterprise. A contact event has a set of identifying parameters. When a contact event is detected, the event's parameters are compared to a set of predetermined values to detect a match. Parameters associated with the contact event can include a name, priority, subject matter, or any set of flags and codes that may resemble a paper-based phone log system. These parameters are then compared with a set of predetermined values, such as a set for detecting or responding to important contact events. If a match exists, then, in response to the contact event, a number of commands are executed according to a predetermined set of at least one rule.

In contrast to the method described by Lapeze et al., amended claims 1, 18, and 23 of the present application, respectively recite, *inter alia*, a method, system and programming device configured to execute steps for managing call reports in a wireless network environment comprising the steps of receiving a message and information regarding a client matter, the message and information providing a summary of an event; determining a distribution list by applying a predetermined set of business rules that encapsulate legal and ethical requirements for allowing access to the client matter, the business rules including restrictions based upon the position of a viewing employee within a company, the matters the employee has worked on, as well as the matters that are within the employee's current responsibility; creating a call report, the call report including the received message; and allowing access to the call report based on the distribution list. The business rule restrictions could best be illustrated by an example. A first restriction can state that the employee must be at a managerial level. This group would include employees A, B, and C. A second restriction states that the managerial employee must have at one time worked on matter Z. This restricted group would include employees A and B but not C. Furthermore, the managerial employee currently works on matter Z. This restricted group would consist only of employee A, since employee B no longer works on matter Z. Therefore, only employee A would be added to the distribution list.

Lapeze et al. does not describe or teach steps for determining a distribution list by applying a predetermined set of business rules including restrictions based upon the position of a viewing employee within a company, the matters the employee has worked on, as well as the matters that are within the employee's current responsibility. In Lapeze et al., a contact event's parameters are compared to a set of predetermined values to detect a match, which can include a name, priority, subject matter, or the like. These parameters are then compared with a set of predetermined values, such as a set for detecting or responding to important contact events. There is no mention of how a person is added to a distribution list for sending a message as encapsulated in a contact event. In paragraph [0007], it is stated that any person with the proper authorization can access any person's contact list, which can include an attorney and the attorney's assistant, but there is no description of how an attorney or their assistant is added to a call list based on business rules. In paragraph [0016] of Lapeze et al., a contact record can be manipulated based on at least one parameter by an authorized user. The authorized user can be the recipient of the contact event, the sender, and a person designated by the sender. None of these people are authorized based on employee position and the matters the employee has worked on, as well as the matters that are within the employee's current responsibility.

Chun et al. fails to correct all of the deficiencies of Lapeze et al. Chun et al. describes an apparatus in the form of an appliance that can be installed in an existing network. The appliance comprises a single modular device that integrates security to allow the appliance to be located at a network gateway where all incoming and outgoing data exchanges must pass through. The appliance, as described, can be installed or plugged into a computer network between business partners, and can perform many of the difficult and tedious data manipulation operations in a secure, transparent, and substantially automated manner. Examples of operations that can be performed include encryption, single sign-on authentication, auditing, shaping data to a common intermediate format for exchange between partners, other auditing of data exchanges in transaction logs, filtering data for privacy compliance and risk management, error detection and correction, mapping internal non-standard data elements to external standard code sets, proxy and protocol re-writing, etc.

Chun et al., either alone, or in combination with Lapeze et al., does not describe or teach all of the steps for determining a distribution list by applying a predetermined set of business rules that include restrictions based upon the position of a viewing employee within a company, the matters the employee has worked on, as well as the matters that are within the employee's current responsibility. At paragraphs [0033] and[0043] of Chun et al., access to "resources" in a system employing the invention of Chen et al. can be based on typical software properties such as username, password, and the software owner of the resource. Access rules can be based upon users/group/machines properties that are typically specified in the operating system of the application. Furthermore, as the Examiner asserts, at paragraph [0054], filtering of who has access to the data can be based on minimum need-to-know rules, such as business security models and mandatory privacy regulations such as HIPPA. There is no further indication or disclosure of what the business rules are, except that it can be based on a minimum need-to-know basis. There is no mention of what criteria establishes an employee as being a person that is included or excluded in the pool of employees that have or have not a "minimum need-to-know." There is also no explicit disclosure in Chun et al. that the appliance of Chun et al. can manipulate a distribution list for a call report based on business rules that have the restriction based on an employee's position in a company, the matters the employee has worked on, as well as the matters that are within the employee's current responsibility.

Stone et al. fails to correct all of the deficiencies of Lapeze et al. and Chun et al. Stone et al. discloses, according to paragraphs [0006]-[0009], a method and an apparatus for managing access to self describing data and for controlling its distribution in a communication network using a directory having one or more objects organized in a hierarchical manner. User access information defines the transmitted content a network user may access. The user access information also defines a format for presenting the accessed content. The user access information is encapsulated into an object of a directory. In addition, attributes of the network user, such as physical location and user preferences (i.e. data content the user wishes to view based on time, date, or dollar amount) are encapsulated into an object in the directory. Additional network user attributes, such as the user's name, I.D., and password, are also encapsulated into an object in the directory. The storing of the objects in the directory enables a user with a valid I.D. and password to electronically access business data from a trading partner, a strategic alliance, or a supplier to perform data analytics on the desired content. The data owner attributes that are encapsulated into an object are defined by the originator and the recipient (the "owner") of the document and provide the properties necessary to control content access for an identified business entity, a business entity location, a user, a group of users, or the like.

At paragraphs [0049] and [0051] of Stone et al., it is stated that data owners may use the various objects of a directory to grant user access to the electronic business transaction content through a combination of attributes such as date of transaction, type of transaction, and trading partners or alliances. Consequently, the data owner may further refine data access based on a specific data element, or documents that meet specific criteria such as total dollar value. The originator and the recipient define the markup language content to be viewed by the destination location such as all transactions above or below a specific dollar amount.

Finally, at paragraph [0054] of Stone et al., it is stated that the interface library combines the originator and the recipient information provided in the document's message header with the business rule objects defined by the owner (the originator and the recipient) of the data in the directory to determine the data content routing instructions. The business rule object may further segregate or define data content authorization for one or more specific users or group of users at the destination location such as a buyer may only view the purchase orders in the commodity class for which they have authorization to purchase, while the head of the purchasing department may have authorization to view all purchase orders.

Nowhere in paragraphs [0006]-[0009], [0049] and [0051] is it stated that access to documents is based on restrictions which include the position of a viewer of the document within an organization. While Stone et al. in paragraph [0054] discloses that the owner of the data or business transaction can define the access rights encapsulated in an object of a directory, and these access rights can be defined down to specific users or groups of users, such as distinguishing between access rights of a buyer versus the head of a purchasing department, which bases the access rule on the position of a person in an organization, not all of the conditions of amended independent claims 1, 18, and 23 are met. More particularly, there is no disclosure or suggestion that, in addition to an employee's position in an organization, access to a document is based also on the matters the employee has worked on, as well as the matters that are within the employee's current responsibility as previously described above.

The Examiner cited U.S. Patent Application Publication No. 2007/0053367 (hereinafter "Tyebji") as being pertinent to the applicant's disclosure. Tyebji discloses that a user can define business rules to determine what information is presented to a user screen, and that, at paragraph [0007] a president of a business can have different access rights than does a warehouse manager. Thus, restrictions to access of documents in Tyebji can be defined according to an employee's position in the company. However, like Stone et al., there is no disclosure in Tyebji that, in addition to an employee's position, access rights also depend on the matters the employee has worked on, as well as the matters that are within the employee's current responsibility.

Accordingly, applicant submits that neither Lapeze et al. nor Chun et al., nor Stone et al., nor Tyebji, alone or in combination, discloses or teaches the invention recited by amended claim 1, 18, and 23 of the present application. Claims 2, and 4-17, and 24-25 ultimately depend from claim 1; and claims 19-22 ultimately depend from claim 18. Since claims 1, 18, and 23 have been shown to be patentable, the claims depending therefrom are likewise deemed to be patentable, for at least the reasons described above with respect to the patentability of claims 1, 18, and 23.

Thus, applicant submits that each of the claims of the present application are patentable over each of the references of record, either taken alone, or in any proposed hypothetical combination. Accordingly, withdrawal of the 35 U.S.C. 103(a) rejections to the claims based on Lapeze et al. in view of Chun et al. and further in view of Stone et al. is respectfully requested.

Conclusion

In view of the above remarks, reconsideration and allowance of the present application is respectfully requested. No fee is believed to be due in connection with this Amendment. If, however, any fees are deemed necessary for this Amendment to be entered and considered by the Examiner, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-1358. Applicant's undersigned patent agent may be reached by telephone at (973) 597-2500. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

Date: 12/4/07

/Raymond G. Cappo/
Raymond G. Cappo
Patent Agent for Applicant
Registration No. 53,836

DOCKET ADMINISTRATOR
LOWENSTEIN SANDLER PC
65 Livingston Avenue
Roseland, NJ 07068